Development of an Improved Access Control System Using a Hybrid Authentication

Sotonwa, Kehinde; Adeyiga, Johnson; Yange, Wilfred; Abass, Olayide
Department of Computer Science and Information Technology,
Bells University of Technology, Ota, Ogun State, Nigeria

Abstract. Data security is indispensable in our society, as human activities are increasingly becoming computerized and are transferred through complex communication networks across the globe. The existing methods used in securing data include cryptography and biometrics. Significant amounts of research have gone into the integration of biometrics with cryptography with the potential to augment access control and secure transmission of sensitive biometric data, it is expected that a robust security system should provide a 100% safety which the world is still far from. On this note, this paper developed an improved access control system using a combination of cryptography and bimodal biometric with emphasis to enhance the techniques such as Advanced Encryption Standard based Fast Fourier Transform (AES-FFT) for encryption and decryption and using Gravitational Search Algorithm (GSA) to elect an optimal feature selection. Five hundred and seventy (570) face and iris images were acquired from iris and face dataset to evaluate recognition accuracy, false positive rate, sensitivity, specificity and average recognition rate time. The developed AES-FFT technique ensured scalable encrypting capacity, good imperceptibility and security performance against various attacks therefore, this vindicate AES-FFT as a better technique in bimodal bio-cryptography with optimal computationally efficiency than existing AES in terms of accuracy and time.

Keywords: Bimodal, Multimodal, Verification, Authentication, Advanced Encryption Standard based Fast Fourier Transform (AES-FFT), Gravitational Search Algorithm (GSA)

Introduction

Access Control System (ACS) is a security system that ensures the physical security of a room or a building, by limiting the access to it, to only specific people and by keeping records of allowed accesses. It utilizes a person-specific authentication method, in order to grant access to specific person. The authentication method using smart card restricts access to only those people who hold an allocated smart card. But the limitations are: difficulty in preventing another person from stealing a legitimate person's card and inconvenience in processing the lost card.

The ACS using a face-based camera device to solve these issues by allowing someone to enter a lecture room or lab only if he punches his thumb on the fingerprinting machine. The detail of entry time can be automatically registered in a database and can be updated on the website, as soon the person enters (or leaves) the room (Mittal *et al.*, 2015). Biometrics access control system has good accuracy for authentication. There were various existing studies about access control system as far as securing the access control system in which most of the studies had mainly aimed to develop an improved prototype (Okokpujie *et al.*, 2018).

Biometric identification is an emerging technology which gains more attention in recent years. It employs physiological or behavioral characteristics to identify an individual (Richard *et al*., 2009; Omidi *et al.*, 2013). The combination of biometric data systems and biometrics recognition/ identification technologies create the biometric security systems. In order to access the biometric security system, individuals need to provide their unique characteristics or traits which match to a database in the system, through this the locking system provides access to the data for the user (Falohun *et al.*, 2016).

Lately, biometric was being integrated with cryptography to alleviate the limitations of the biometric or cryptography system. Biometric is the unique measure of the identity of

individual with their behavioral and physiological traits like face, fingerprint, iris, retina, palm-print and speech. As biometric is directly linked with the owner, it removes the problem to memorize the cryptographic key and confirms the non-repudiation of users (Jain *et al.*, 2013). The authentication systems which integrate biometric traits with cryptography are called crypto-biometric systems (Hao *et al.*, 2012).

Multimodal biometric Fusion has achieved significant attention in few years because it increases the performance of system. Cryptography with multimodal biometric improves the security of the system. There are two type of cryptography technique: symmetric key and asymmetric key cryptography technique. In symmetric key cryptography, same key is used for encryption and decryption process. Symmetric key based Advanced Encryption Standard (AES) algorithm have been used recently (Komal, 2019). This work involves a combination of cryptography technique and bimodal biometric is developed using an Advanced Encryption Standard based Fast Fourier Transform (AES-FFT) and bimodal biometric. Face and iris were used as the two biometric traits for authentication. Features are extracted using Principal Component Analysis (PCA) and fusion is done at feature-level using Weighted Average and finally, optimal features were selected using Gravitational Search Algorithm (GSA).

Review of Related Works

Jagadeesan *et al.*, (2010) proposed an approach based on multimodal biometrics using fingerprint and fingerprint images to generate a protected cryptographic key. In their study, security is further improved with the difficulty of factoring large numbers. In a view to achieve this, minutiae points and texture properties were extracted from the fingerprint and fingerprint images respectively. At the feature level, the extracted features were fused to obtain the multi-biometric template and a multi-biometric template was used for generating a 256-bit cryptographic key.

Selvarani and Visu (2015) presented personal identification using fingerprint and iris biometric technology. Usually unimodal biometric techniques were used. Cloud computing provides many resources, very convenient charged service and minimum cost computing. The existing unimodal bio cryptography techniques often have limitations such as consciousness to noise, intra class consistency, data aspect and other factors. Combined biometric technology will secure the data from unauthorized users.

Oluwadamilola *et al.*, (2017) presented combination of cryptography and biometrics; a bimodal biometric cryptosystem, using fingerprint and face as trait for authentication. Subjects' information was encrypted using Advanced Encryption Standard (AES) and biometric templates were stored as Binary Large Object (BLOB) in MYSQL database secured with Message Digest 5 (MD 5) Hashing Algorithm. The system was developed and implemented to operate on one-try, two-try and three-try configurations at varying threshold values. The developed system's performance was evaluated using False Reject Rate (FRR), False Accept Rate (FAR) and Receiver Operating Characteristic Curve (ROC) graph as performance metrics. On ROC graph, three-try configuration gave optimal performance at all threshold values.

Okokpujie *et al.*, (2018) proposed bimodal biometrics (fingerprint and iris) as a means of ensuring the full integrity of the bank's vault system, thus, further reducing the rate of compromise and theft within the bank's vault system. The accuracy of the system is measured in terms of sample acquisition error and recognition performance using False Accept Rate (FAR), False Identification Rate (FIR) and False Reject Rate (FRR). The result showed that the proposed system was very effective. Komal (2019) studied a robust multimodal biometric crypto system, in which two modalities (FKP and face) were used for authentication of a person and one modality (fingerprint) was used for key generation. AES algorithm with fingerprint-based key was used for securing the biometric templates. The proposed multimodal biometric

crypto system was more robust and secure as compared with other multimodal biometric systems.

Methodology

Gravitational Search Algorithm (GSA) is a heuristic optimization algorithm proposed by Rashedi *et al.*, (2009) based on the gravitational law and laws of motion. The GSA is a nature inspired algorithm which uses the theory of Newtonian physics and its searcher agents are the collection of masses. GSA is used to improve the particle utilization in the search space and works efficiently like the algorithms with memory, therefore this makes it memory less algorithm. Figure 1 below depict flowchart of standard GSA respectively.

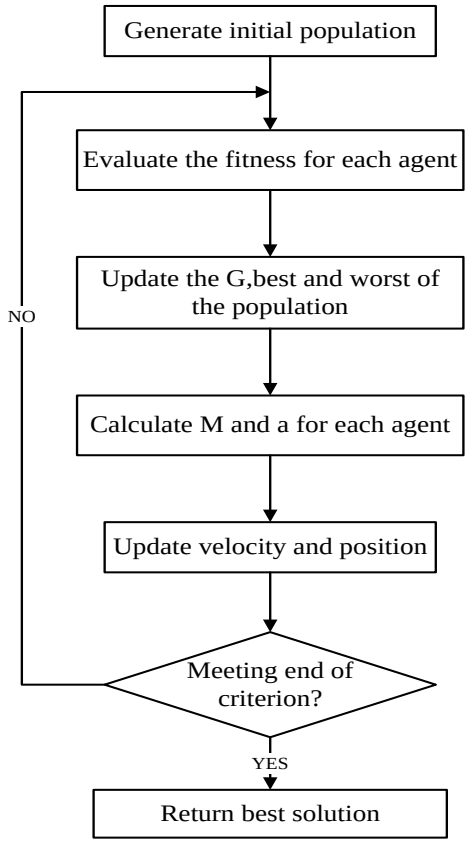


Figure 1: The Gravitational Search Algorithm Flowchart (Rashedi *et al.*, 2009)

Feature Selection Using Gravitational Search Algorithm

The procedural test for achieving a feature selection with GSA are as follow:

Step 1: Agents initialization
Step 2: Fitness evolution and best fitness computation
Step 3: Gravitational constant (*G*) computation
Step 4: Calculation of the Masses of the agents
Step 5: Calculation of Agent's Accelerations-
Step 6: Velocity and positions of agents.

Encryption and Decryption Module

The biometric information submitted in the database are encrypted using Advanced Encryption Standard with Fast Fourier Transform (AES-FFT) cryptography algorithm. This is to safeguard that subject biometric information is not saved in its original or plain biometric

form in order to enhance the system security. AES-FFT algorithm works on the principle of substitution permutation network.

The following steps are used for encryption and decryption:

Step 1: Derive the set of round keys from the cipher key.

Step 2: Initialize the state array with the block data (plaintext).

Step 3: Add the initial round key to the starting state array.

Step 4: Performance nine rounds of state manipulation.

Step 5: Perform the tenth and final round of state manipulation.

Step 6: Copy the final state array out as the encrypted data (cipher text).

Step 7: Each round of the encryption process requires a series of steps to alter the state of array. These steps involve four types of operations namely: Subbytes, Shiftrows, Mixcolumns and Xorroundkey.

AES-FFT

Fast Fourier Transform was applied on the image I(x,y) to obtain FFT coefficients of the images. The image features after application will contain the real part, imaginary part, and magnitude value. FFT was used as modification factor on shift row transformation step and on mix column transformation of AES algorithm. The basic structure of the modification process is described in Figure 2 and every other steps of AES algorithm remain the same, except that some modification was made at “ShiftRows” and “MixColumn” level using FFT.

Shiftrows

If the element of first row and first column is even, then first and fourth row remain unchanged and each byte in the second and third row of the state is cyclically shifted right over different number. If the element of firs row and first column is odd, then first and third row remain unchanged and each byte in the second and fourth row of the state is cyclically shifted right over different number.

Mixcolumn

In the mix column the 128-bit arranged as a 4*4 state matrix are operated column by column. The four elements of each column form a five-term polynomial that is multiplied by constant polynomial $A(Y) = \{03\}X^4 + \{01\}X^3 + \{01\}X^2 + \{01\}X + \{02\}$ with module X^5+1 gets the new state matrix. After getting the state matrix from step 1 then interchanging the rows and column of the matrix.

Performance Evaluation

In this research work the performance of Support Vector Machine (SVM) was done using Recognition Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and Computation Time.

False acceptance rate (FAR)

This is the percentage of times in which the system accepts an unauthorized user. FAR describes the rate at which imposter are incorrectly accepted as genuine person.

A false acceptance may result to a damage imposter which are incorrectly accepted as genuine person. A false acceptance may lead to damage when matching score established by a biometric system for an imposter to satisfy the threshold criteria of matching. It is also referred to as False Match Rate (FMR).

$$FAR = \frac{\text{number of impostors accepted (FP)}}{\text{Total number of imposter comprisons (TN+FP)}} * 100\% \quad (1)$$

False rejection rate (FRR)

FRR is the percentage of times the system rejects an authorized user. i.e. FRR is the rate at which a genuine person is correctly rejected as an imposter. It is also called False Non-Match Rate (FNMR).

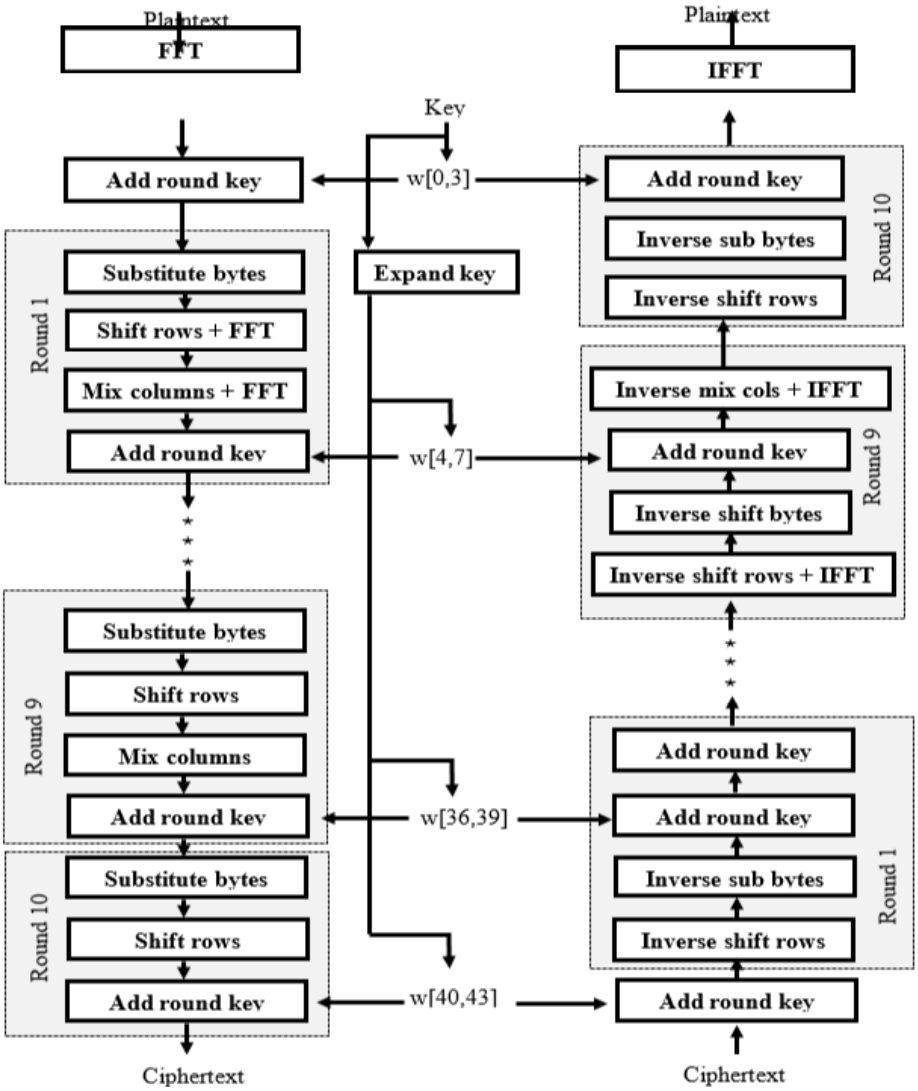


Figure 2: Basic Structure of AES-FFT

$$FRR = \frac{\text{Number of genuine person rejected (FN)}}{\text{Total number of genuine comparism (TP+FN)}} * 100\% \quad (2)$$

Recognition accuracy (RA)

RA is used to measure the performance of a verification system. It is defined as:

$$RA = \frac{(\text{TP+TN})}{(\text{TP+FN})} * 100\% \quad (3)$$

Result and Discussion

The AES (GSA) and AES-FFT (GSA) model were experimented by implementing the face and iris expression recognition using 128 by 128-pixel resolution. All performance metrics were analyzed using a square dimension pixel resolution at different threshold values. Three hundred and forty-two (342) face and iris images were used for training which equal to 60% of the total dataset and two hundred and twenty-eight (228) face and iris images which equivalent to 40% of the total dataset were used for testing. Figures 3-5, showed the GUI training phase of iris and face and Table 1-2 revealed the results of fused iris and face with AES (GSA) and AES-FFT (GSA), while Table 3 displayed the comparison of the result generated from the experiment.

The fused iris and face gave 97.81%, iris had 94.74% and face 96.49% recognition accuracies with AES-FFT (GSA) respectively. While, the fused iris and face gave 95.61%, iris

Figure 3: Graphical user interface (GUI) showing training phase sample of iris

Figure 4: Graphical User Interface (GUI) showing training phase sample of face and iris

Figure 5: Graphical user interface (GUI) showing training phase sample of face and iris

had 92.11% and face 92.54% recognition accuracies with AES (GSA) respectively. It can be inferred from the results of the performance metrics that AES-FFT (GSA) applied with iris and face gave the best result. In view of the above results, fused iris and face with AES-FFT (GSA) gave more accurate due to high number of true positive as well as low number of true negative leading to high accuracy.

Table 1: Fused Iris and face with AES results

TP	FN	FP	TN	FAR (%)	FRR (%)	ACC (%)	Time (sec)	Threshold
166	5	9	48	15.79	2.92	93.86	552.70	0.20
165	6	7	50	12.28	3.51	94.30	561.42	0.35
164	7	5	52	8.77	4.09	94.74	562.14	0.50
163	8	2	55	3.51	4.68	95.61	565.02	0.76

Table 2: Fused Iris and face with AES-FFT results

TP	FN	FP	TN	FAR (%)	FRR (%)	ACC (%)	Time (sec)	Threshold
170	1	9	48	15.79	0.58	95.61	418.27	0.20
169	2	6	51	10.53	1.17	96.49	426.35	0.35
168	3	3	54	5.26	1.75	97.37	436.18	0.50
167	4	1	56	1.75	2.34	97.81	455.54	0.76

Table 3: Comparison of AES (GSA) and AES-FFT (GSA) at 128 by 128-pixel resolution at 0.76 threshold value

Algorithm	TP	FN	FP	TN	FAR (%)	FRR (%)	ACC (%)	Time (sec)	Threshold
AES-FFT (GSA)	167	4	1	56	1.75	2.34	97.81	455.54	0.76
AES (GSA)	163	8	2	55	3.51	4.68	95.61	565.02	0.76

Conclusion

The experimental results obtained revealed that the fused iris and face under AES-FFT encryption technique with SVM gave 97.81% in terms of recognition accuracies, 1.75% false acceptance rate, 2.34% false rejection rate, and 455.54s recognition time compare with iris and face modality. In view of this, an automated bi-modal bio-cryptography system based on fused iris and face (that is, both face and iris), would produce a more reliable accuracy and secure bi-modal bio-cryptography system on any repository system as a result of its high accuracy. In other words, the developed AES-FFT technique has ensured scalable encrypting capacity, good imperceptibility and security performance, and robustness against various attacks with optimal computationally efficiency in terms of its accuracy and time.

References

Mittal, Y., Varshney, A., Aggarwal, P., Matani, K., & Mittal, V. K. (2015). Fingerprint Biometric based Access Control and Classroom Attendance Management System. Annual IEEE India Conference *(INDICON)*, 1-6.

Okokpujie, K. O., Odusami, M., Noma-Osaghae, E., Abayomi-Alli, O., & Oluwawemimo, E. (2018). A Bimodal Biometric Bank Vault Access Control System. *International Journal of Mechanical Engineering and Technology (IJMET), 9*(9), 596-607.

Richard, P. J., Devinney, T. M., Yip, G. S., & Johnson, G. (2009). Measuring Organizational Performance: Towards Methodological Best Practice. *Journal of Management, 35*(3), 718-804.

Omidi, A., Mohammadkhani, P., Mohammadi, A. & Zargar, F. (2013). The Effectiveness of Combined Mindfulness-Based Cognitive Therapy with Cognitive Therapy and Classical Cognitive-Behavioural Therapy in Reducing Dysfunctional Attitudes of Patients with Depressive Disorders. *Scientific Journal of Birjand University of Medical Sciences, 20*, 383-392.

Falohun, A. S., Fenwa, O. D., & Oke, A. O. (2016). An Access Control System using Bimodal Biometrics. *International Journal of Applied Information Systems, 10*(5), 41-47.

Jain, A. K., Nandakumar, K. & Nagar, A. (2013). *Fingerprint Template Protection: Security and Privacy in Biometrics*. London: Springer, 187–214.

Hao, N., Yildirim, N., Nagiec, M.J., Parnell, S.C., Errede, B., Dohlman, H.G., & Elston, T.C. (2012). Combined Computation and Experimental Analysis Reveals Mitogen-activated Protein Kinase-mediated Feedback Phosphorylation as a Mechanism for Signalling Specificity. *Mol Biol Cell, 23*(19), 3899-910.

Komal, C. K. (2019). A Robust Multimoel Biometric Crypto System. *International Journal of Recent Technology and Engineering (IJRT), 8*(2S8), 1953-1961.

Jagadeesan, T., Thillaikkarasi, T., & Duraiswamy, K. (2010). Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature. *International of Journal of Computer Applications, 2*(6), 16-26.

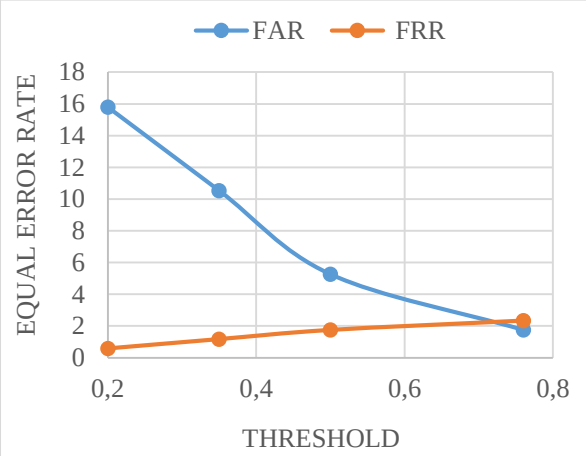
Selvarani, P., & Visu, P. (2015). Multi-model Bio-cryptographic Authentication in Cloud Storage Sharing for Sigher security. *Research Journal of Applied Sciences, Engineering and Technology, 11*(1), 95-101.

Oluwadamilola, K. O., Ayodeji, A. O., Martins, O. O., Olufunmi, I. S., & Rapheal, O. A. (2017). An Improved Authentication System using Hybrid of Biometrics and Cryptography. *IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, 457-463.

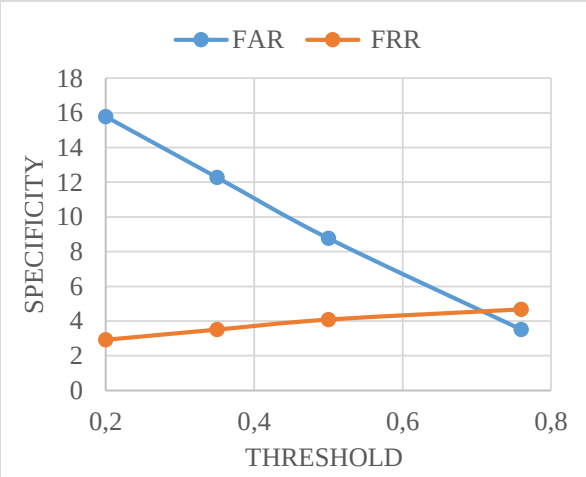
Okokpujie, K. O., Odusami, M., Noma-Osaghae, E., Abayomi-Alli, O., & Oluwawemimo, E. (2018). A Bimodal Biometric Bank Vault Access Control System. *International Journal of Mechanical Engineering and Technology (IJMET)*, *9*(9), 596-607.

Rashedi, E., Nezamabadi-pour, H., & Saryazdi, S. (2009). GSA: A Gravitaional Search Algorithm, Department of electrical Engineering, Shahid Bahonar University of Kerman, Iran, Information Sciences, ELSEVIER, 2232-2248.

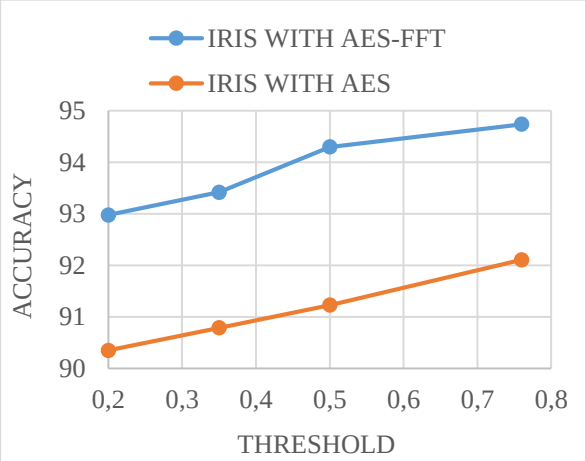
Appendixes



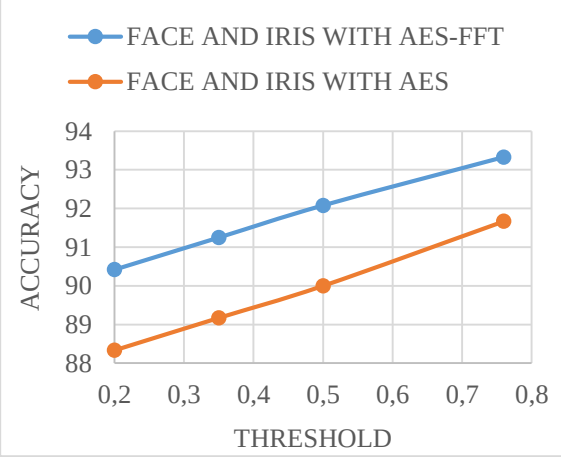
Appendix 1: Graph showing equal error rate of 2.05 with face and iris under AES-FFT



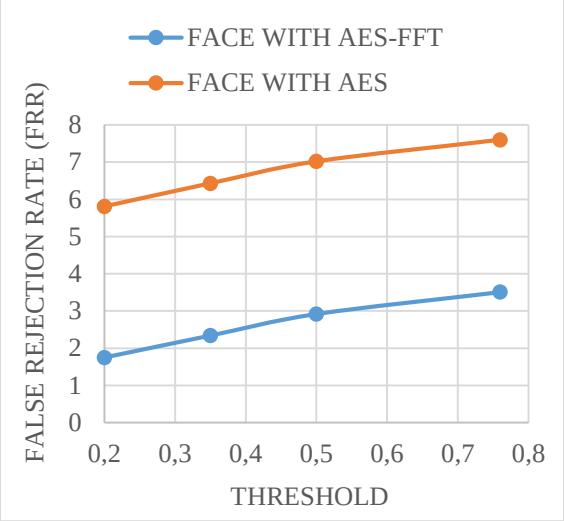
Appendix 2: Graph showing equal error rate of 4.09 with face and iris under AES



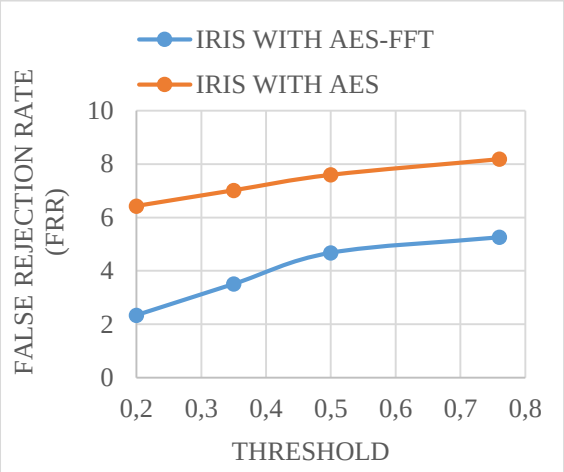
Appendix 3: Graph showing Accuracy with Iris



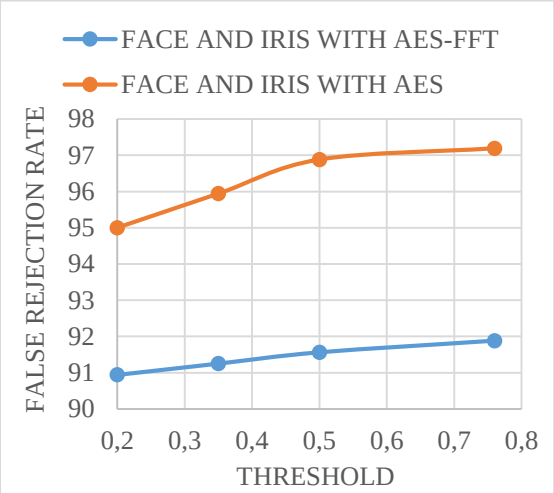
Appendix 4: Graph showing Accuracy with Face and Iris



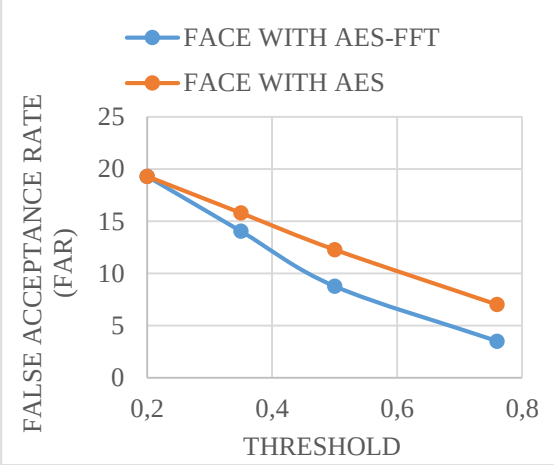
Appendix 5: Graph showing False rejection rate (FRR) with face



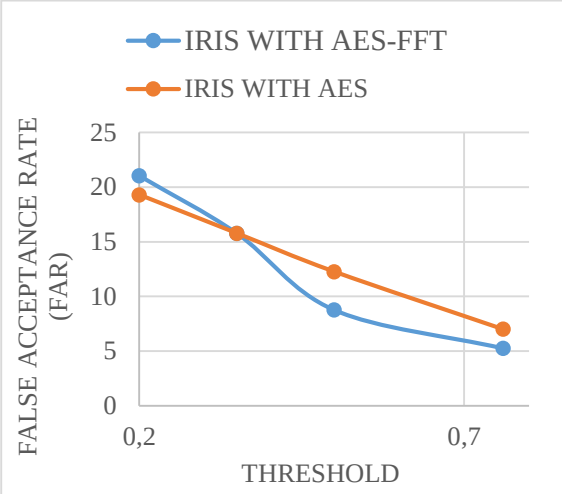
Appendix 6: Graph showing False rejection rate (FRR) with iris



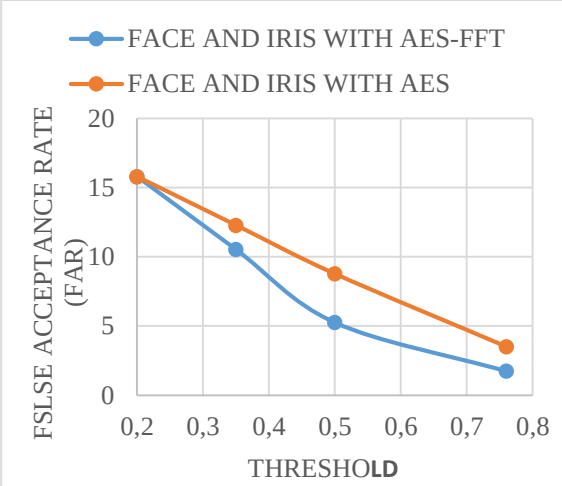
Appendix 7: Graph showing False rejection rate (FRR) with face and iris



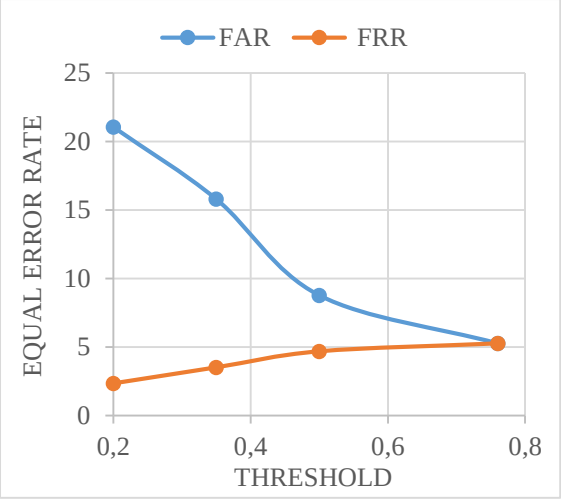
Appendix 8: Graph showing False Acceptance rate (FAR) with face



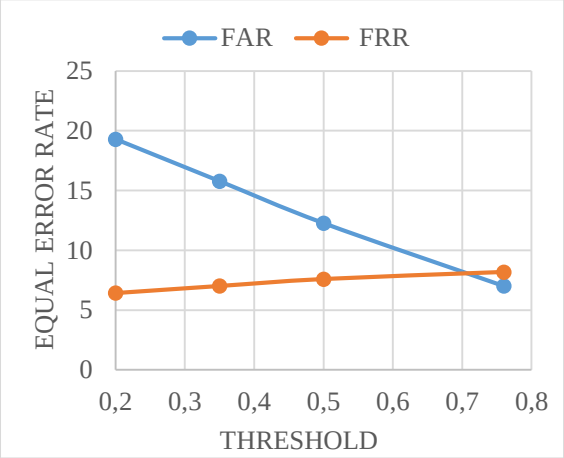
Appendix 9: Graph showing False Acceptance rate (FAR) with iris



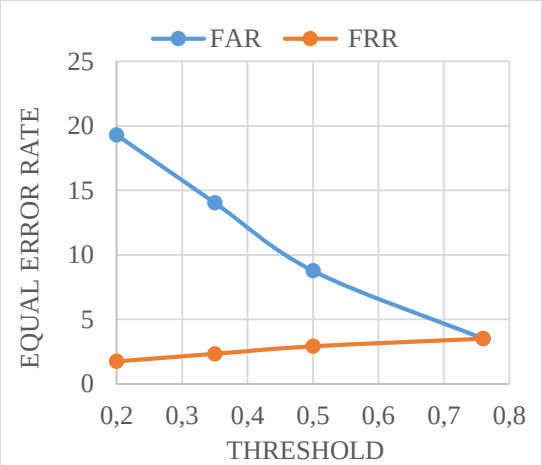
Appendix 10: Graph showing False Acceptance rate (FAR) with face and iris



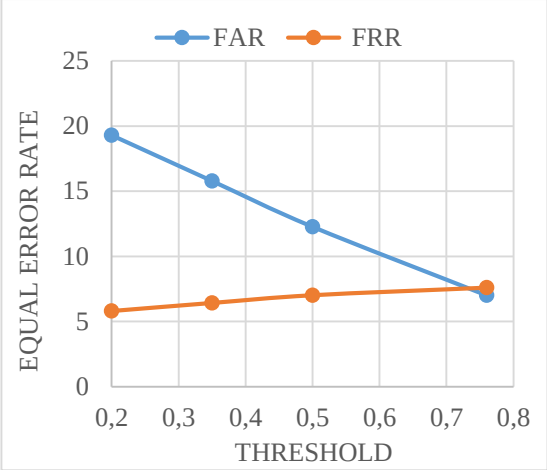
Appendix 11: Graph showing equal error rate of 0.8 with iris under AES-FFT



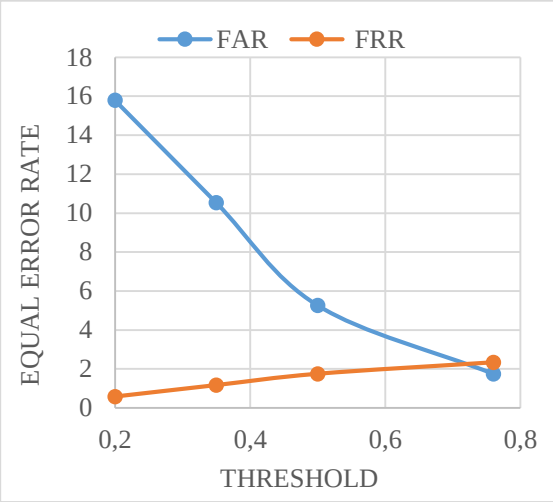
Appendix 12: Graph showing equal error rate of 7.9 with iris under AES



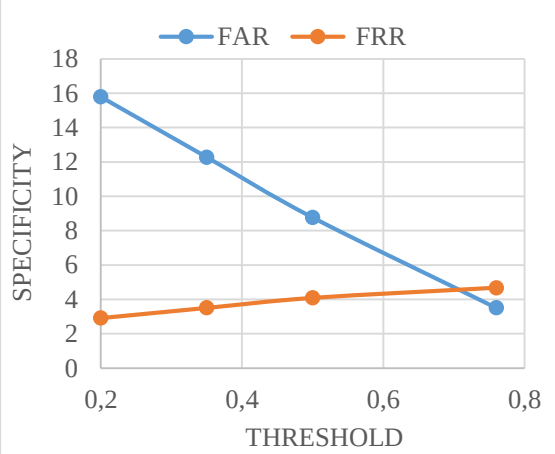
Appendix 13: Graph showing equal error rate with face under AES-FFT



Appendix 14: Graph showing equal error rate of 7.01 with face under AES



Appendix 15: Graph showing equal error rate of 2.05 with face and iris under AES-FFT



Appendix 16: Graph showing equal error rate of 4.09 with face and iris under AES